## In The Specification

Please replace the paragraph beginning on page 14, line 1 with the following rewritten paragraph.

Prior to encrypting the message M, a check is made to determine whether the numerical or binary value of the message M is equal to or greater than the sender's modulus  $N_A$  (block 106). If the numerical value of message M is equal to ergreater or greater than the sender's encryption modulus  $N_A$ , the message M would be reduced during the encryption operation by subtraction of the modulus  $N_A$  resulting in data loss. Therefore, when message M is greater than the sender's modulus  $N_A$ , the bit occupying the MSB position is changed to 0 (block 110). This ensures that modulus  $N_A$  has a greater numerical value and that data will not be lost during the encryption operation. The possibly modified message M is then signed using the sender's private key  $K_{PRIVA}$  and encryption modulus  $N_A$  (block 112) to create a once encrypted bitstring. If the RSA algorithm is used, encryption is performed using the equation  $Y = M_A^{K_{PRIVA}}$  mod  $N_A$ , where Y is the signed message. The signed message Y is encrypted at step 114 using the recipient's public key  $K_{PUBB}$  and encryption modulus  $N_B$  to create a doubly-encrypted bitstring. Again, if the RSA algorithm is used, the encryption operation is performed using the  $Z = Y_A^{K_{PUBB}}$  mod  $N_B$  where Z is the encrypted message. The encrypted message Z is then transmitted by the sender to the recipient (block 116).